

Teoría de las Comunicaciones

22 de Noviembre de 2023

2^{do} Recuperatorio



Departamento de Computación
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Apellido:	LU:	Hojas ->	Ej.1	Ej.2	Ej.3	Ej.4	Ej.5	
Basilio	108/20		B-	B	B	B+	R	A
Nombres:		Calif. ->	1	1	1	1	1	Final:
Ramiro								

Todas las respuestas se consideran válidas solo si están debidamente justificadas.

Ejercicio 1

Como se muestra en la lista de segmentos TCP, ambos hosts inician la conexión al mismo tiempo. Explicar por qué estados pasan ambos extremos de la conexión y continuar la secuencia de segmentos hasta que se cierre la conexión de manera que ambos hosts pasen por la misma secuencia de estados. Suponer que los hosts no se envían datos.

Origen	Destino	FLAGS	#SEQ	#ACK	Largo
B	A	Syn	3333	-	-
A	B	Syn	4444	-	-
A	B	Syn+Ack	4444	3334	-
B	A	Syn+Ack	3333	4445	-

Ejercicio 2

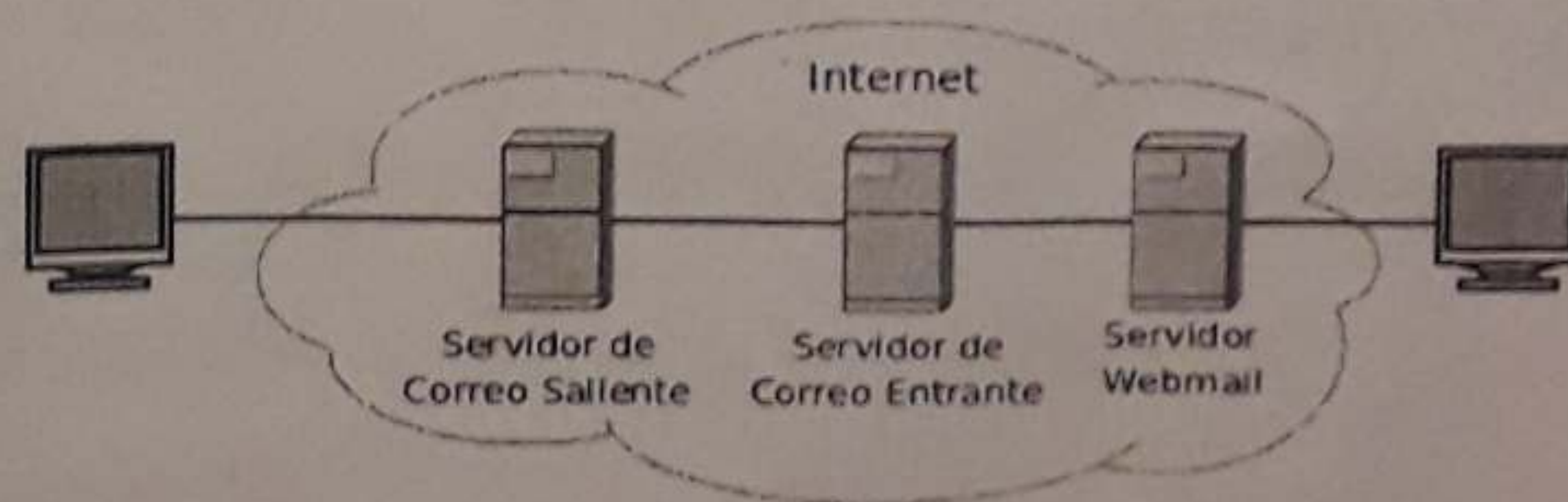
En una conexión recién establecida con $RTT=100ms$ el receptor siempre anuncia una *Advertised Window* de 64KB. A su vez, el proveedor de servicio descarta los paquetes de la misma si una ráfaga fuera de 12KB o mas. ¿Cuáles son los valores finales de CWND y SSTHRESH después de enviar 50KB de datos?

Ejercicio 3

Peterson y Tanenbaum desean comunicarse por correo electrónico utilizando direcciones de correo personalizadas. Sus direcciones son `claudio@peterson.com` y `ernesto@tanenbaum.com`. Describa los registros DNS necesarios en las zonas de dominio `peterson.com` y `tanenbaum.com` para que puedan enviarse y recibir correos. Suponer que la descarga de los correos es por medio del protocolo POP3.

Ejercicio 4

Como se indica en la figura, un usuario en una PC envía un correo en texto plano, usando un *User Agent* a un usuario que accede a su correo usando *Webmail*. Suponiendo que el servidor Webmail usa POP3 para descargar los correos desde el servidor entrante, explicar cuántas conexiones TCP se abren y qué protocolos transportan desde que se envía el correo hasta que el usuario lo visualiza en su computadora.



Ejercicio 5

Los servidores de un sistema distribuido necesitan comunicarse a través de Internet garantizando su AUTENTICIDAD entre sí (los servidores todos contra todos) y para eso usan SSL/TLS para comunicarse. Suponiendo que la compañía dispone de un certificado digital firmado por una autoridad certificante, explicar dónde deberían instalarse los certificados digitales y por quién deberían estar firmados.

Ejercicio 1

B=

Orig	Dest	Flags	#seq	#ack
B	A	S	3333	-
A	B	S	4444	-
A	B	SA	4444	3334
B	A	SA	3333	4445
---	---	---	---	---
B	A	F	3334	4445
A	B	F	4445	3335
A	B	A	4445	3335
B	A	A	3334	4446
A	B	A	4445	3335

2) A y B se encuentran inicialmente en el mismo estado closed, por lo que tienen que iniciar la conexión en simultáneas. ~~B manda un~~

B avanza mandando un SYN y pasa a SYN-SENT.
A, ~~que aún no~~ ~~re recibió~~ recibió el SYN de B, ~~mandando~~ su propio SYN para pasar a SYN-SENT.
~~Cuando recibe el SYN de~~

Cuando A recibe el SYN de B responde un SYN+ACK para pasar a SYN-RCVD. Luego B, habiendo recibido el SYN de A, contesta SYN+ACK para pasar también a SYN-RCVD.

X Falta un ACK para que ambos pasen de SYN-RCVD a ESTABLISHED.
b) ~~Simultáneamente~~ 2) B manda un FIN primero y pasa a FIN-WAIT-1.

A lo recibe y contesta con su propio FIN para ~~T pero no~~ el SA

Ejercicio 2

RTT	CWND	RWND	SSTH	FS	LBS	LBA
1	4	64	64	4	4	0
2	8	64	64	8	12	4
3	16	64	64	16	28	12
4	16	64	64	0	28	12
5	2	64	8	2	14	12
6	4	64	8	4	18	14
7	8	64	8	8	26	18
8	10	64	8	10	36	26
9	12	64	8	12	48	36
10	12	64	8	0	48	36
11	2	64	6	2	38	36
12	4	64	6	4	42	38
13	18	64	6	8	50	42
14	8	64	6	1	50	42

No recibió ACK, TO,
 $SSTHRESH = FS/2$, reinicio CWND

No recibió ACK, TO
 $SSTH = FS/2$, reinicio CWND

$(CWND + 2) = 6$ con un ACK
 y ahora, para los 3 ACK
 restantes, se usa CA, luego
 $(CWND + 3 \cdot (2 \cdot 2 / 6)) = 8$

Los valores son 8 y 6 respectivamente.

Falta que lleguen los ACKs

Arranca con slow start hasta que Flight size excede 12 KB, lo que causa que el receptor descarte todo, no vienen ACKs (CWND queda fijo) y finalmente TO.

El TO hace que CWND venga a 2 y $SSTHRESH$ baje. Continúa slow start hasta que vuelve a suceder lo mismo y termina en TO.

B

Ejercicio 3

Las zonas de ambos dominios realmente solo necesitan MX para enviar y recibir correos, que es el registro que mandan a buscar SMTP y POP3

En peterston.com. (su dns)

peterston.com. IN MX {ip del mail server}

En tanenbaum.com: (su dns)

tanenbaum.com. IN MX {ip del mail server}

Asumiendo que ambos tienen un mail server con respectivos servicios SMTP y POP3.

La autoridad de zona .com. va a necesitar un par de records NS apuntando a ~~las~~ direcciones los name servers que manejan cada dominio respectivamente.

B+

Camilo Basile

108/20

Ejercicio 4

La PC necesita una conexión TCP con el sv. saliente para comunicarle por SMTP el mail que quiere enviar, ~~intercambiando~~ mandando HELO, MAIL TO, RCPT TO, DATA ... ✓

El servidor saliente necesita ~~formar~~ replicar esta conversación con el servidor entrante a través de SMTP, por lo que se necesita una conexión TCP entre ellos. ~~El servidor~~
~~POP3 que proporciona~~ ✓

Cuando un usuario accede a su webmail desde su navegador a través de HTTP. Asimismo HTTP / 1.1 o más, se necesita una única conexión TCP entre el sv. webmail y la compu donde está el navegador. ✓

El contenido de la página webmail tienen que ser los mails del usuario, por lo que el sv. webmail primero necesita travesarse antes de poder contestar el request HTTP del usuario. Esto lo hace comunicándose con el ~~sv.~~ sv. entrante a través de POP3, lo que requiere otra conexión TCP. ✓

Ejercicio 5

Cada servidor tiene que tener un certificado firmado por la autoridad certificante y tiene que conocer la llave pública de la autoridad.

Para el handshake SSL/TLS, quien inicia la conexión recibe un certificado y con la llave pública de la CA verifica que sea auténtico. Esto garantiza la AUTENTICIDAD de uno al otro, pero ~~se~~ tiene que hacerse el proceso en dirección contraria para garantizar AUTENTICIDAD todos contra todos.

Es necesario que identifique al host emisor (en este caso, como es un solo cert., a todos los hosts) cosa de que solo sirva en manos de ese host.

Unos \rightarrow obtener

¿cuál es la autoridad? \rightarrow nunca dice certificado de la compañía

¿cómo se obtienen los certificados?

¿cómo se demuestran los certificados?